MEV and EIP-1559

Kristof Gazso (Nethermind) & Alejo Salles (Flashbots)

The incorporation of EIP-1559 in the London hardfork brings a major restructuring of the Ethereum fee mechanism, aiming to allow for easier fee estimation by users and consolidate ETH as the base currency of the network by burning part of the transaction fees. This post analyzes some of the consequences of this EIP under the light of the MEV (Maximal Extractable Value) phenomenon, that is, the permissionless extraction of value by the reordering, addition, or censoring of transactions.

Under the new fee mechanism, instead of choosing a gas price for their transactions, users set a "priority fee" for miners to incentivize inclusion, alongside a "max fee", stating the absolute maximum price that they are willing to pay. The protocol will now set a per-block "basefee", computed programmatically from the amount of gas used in the block immediately before, in a negative feedback loop meant for block sizes to stabilize around a target size s_0 (initially equal to the maximum current block size). Valid transactions pay a gas price equal to the basefee plus the priority fee (only up to the max fee--needed in case of sudden basefee increases); the priority fee goes to the miner, and, crucially, the basefee is burnt.

These changes have some obvious immediate implications for MEV-related infrastructure, like eliminating the possibility of zero-Gwei transactions, which are presently used for front-running protection in some DEXes like MistX, where miner fees are taken directly from the transferred tokens. On the other hand, we don't expect radically new sources of MEV to arise from the novel fee mechanism. In this note, we highlight three areas where EIP-1559 might have interesting consequences for MEV: increased MEV extraction incentives for miners, the coexistence of different auctions in the Ethereum protocol and its implications for EIP design, and the role of Flashbots as a miner coordinating agent and its ethical implications.

## Miners economics and the increased incentive for MEV extraction

Either due to proper economic incentives or because of their loyalty to the network, miners have produced blocks since the inception of Ethereum without major malicious deviations from the protocol. The Flash Boys 2.0 paper however warned of the nefarious consequences that indiscriminate MEV extraction might bring to the protocol like transaction censoring, or chain re-orgs ultimately threatening consensus stability. Notably, however, it was only recently that MEV extraction became the standard for miners when Flashbots introduced MEV-geth, a fork of the geth client that miners can run to start receiving "MEV bundles", packaged sets of transactions that ensure a payment to miners upon inclusion. Partly due to the looming threat of EIP-1559 reducing their income, most miners were quick to adopt MEV-geth to partially palliate the shock. It is then reasonable to ask, when EIP-1559 comes into action, whether miners will devote extra efforts for further MEV extraction, in particular in ways that are harmful to the network.

While we are not able to make a quantitative prediction due to the hard to quantify loyalty component, we find it useful to be able to think of MEV extraction on the same footing as other strategies miners have to compensate for lost revenue, like switching their hashrate to other GPU chains. To this effect, we provide a basic model of miner economics allowing us to estimate the required increase in Realized Extractable Value[^rev] to match the profit hike from switching chains post-London.

We start by defining a set of Proof-of-Work GPU-based chains X excluding Ethereum where miners could (we assume costlessly) point their hashrate to. We then posit that, in equilibrium, total GPU hashrate H will be distributed between Ethereum (pre- and post-London) and X in a way that maximizes profit-per-hashrate (otherwise more miners would switch until this equilibrium is attained). Finally, assuming cost-per-hashrate is constant and the same for all chains, we can derive the hashrate fraction that will remain in Ethereum after the London hard fork. This can be succintly expressed as:

$$\frac{H_{1559}}{H_E}=\frac{1+\delta}{1+\delta/\gamma},$$

where H_{1559} is the post-London Ethereum hashrate, H_E is the pre-London Ethereum hashrate, $\gamma=\frac{R_{1559}}{R_E}$ is the fraction of total revenue left for miners in Ethereum after EIP-1559, and $\delta=\frac{R_X}{R_E}$ is the ratio of total X revenues to pre-London Ethereum revenues (we save the reader from the algebra, which can be checked here). The relation between these quantities can be visualized as follows:
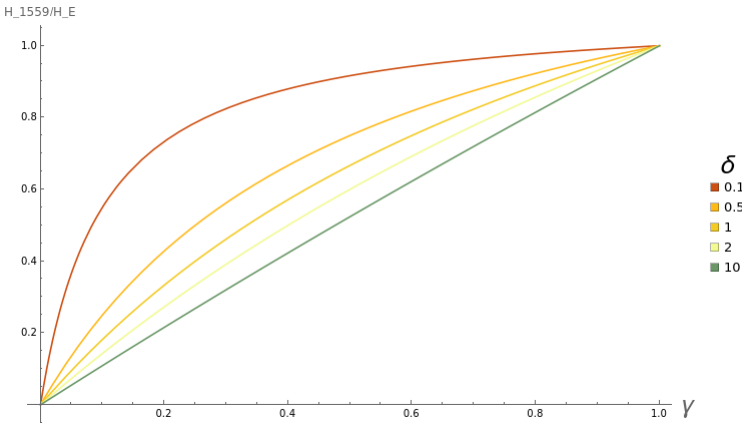
Gas prices in Ethereum have suffered variations of two orders of magnitude, which makes it extremely hard to produce accurate estimations for the parameters of the model. We can still use data from the Flashbots dashboard and Etherchain's data on mining reward to pick a value of $\gamma=0.86$ for the fraction of total miner revenues that will still be available in Ethereum after EIP-1559, based on recent gas prices. Finally, using CoinMetrics data to find the mining revenue in USD per day for GPU-based PoW chains other than Ethereum to find R_X, we get an approximate value of $\delta=0.15$[^xchains]. Plugging in these value we obtain $\frac{H_{1559}}{H_E}\simeq 98\%$ for the fraction of hashrate staying in Ethereum after the London fork[^numbersused].

This constitutes an extremely simplified model of miner economics, neglecting in particular the cost of switching to other chains. It does however provide a framework to reason about MEV revenues in the broader context of miner economics. Based again on highly-varying Flashbots data, we find that, all other things being equal, the fraction of miners' revenue coming from Realized Extracted Value will rise from 2.9% pre-London to 3.4% after the fork[^basefee]. If, instead of switching their hashrate to other chains until attaining equilibrium miners decided to compensate for the reduced revenue by extracting more MEV, it would take them an extra 22% of extracted MEV to match the profit hike of switching lanes (which would still entail a great revenue reduction from the pre-London rates). A more detailed model including an explicit formulation of the costs of extra MEV extraction vs. chain switching is outside the scope of this note. The wildly varying nature of the values involved casts some doubt about the utility of highly elaborate models, on top of the subjective factor of miner loyalty playing a big part in miners' course of action.

On this note, most mining pools have publicly opposed the EIP, feeling that they are being thrown under the bus after half a decade of maintaining Ethereum's security. Tim Roughgarden's analysis of EIP-1559 points out that miner loyalty might be a major reason why there haven't been any major disruptions to Ethereum's consensus since genesis, even if deviations from the protocol might have temporarily yielded increased profits. This might make a decrease in miner revenue that arises from the implementation of this EIP more dangerous than if it came from a drop in the price of ETH, since it comes accompanied by a loss of trust on the miners' side. Ultimately, we will need to wait until the EIP goes live to see the extent to which miners start going to extra lengths to extract more MEV in ways detrimental to general network health, as we discuss later in the post.

Many auctions in one

The fee mechanism put forth in EIP-1559 was designed (and later analyzed) with an auction for transaction *inclusion* in mind. In fact, however, much of the activity in Ethereum is concerned with not only inclusion but also transaction *ordering* within a block. Most MEV extraction opportunities depend on the relative positioning of transactions, just having transactions included won't cut it. The current first-price mechanism is limited in that users can express their wish to be included earlier than a certain target transaction, or, at most, aim at landing just after one by picking its exact gas price and hoping luck will be in their favor (backrunning). This limitation has led to systems like Flashbots, which provide a richer language for expressing preferences (users can bid for precise relative ordering of transaction sets, the "MEV bundles" mentioned above).

Another desirable property not provided by the current pricing mechanism is *privacy*. Searchers extracting MEV typically wish their maneuvers to be kept private--at least until they are inevitably made public when mined in a block--to prevent other actors from stealing their lot. Flashbots, as well as other private pool providers, offer this kind of guarantee (apart from uncle risk or miner misbehavior). Recently, several user-facing applications like MistX and 1inch have turned to Flashbots to provide users front-running protection in their trades. If an increasingly larger fraction of the network is concerned with bidding for ordering and privacy as opposed to simply inclusion, this begs the question whether EIP-1559 brings any advantage at all, or will instead be entirely superseded by Flashbots-like, more expressive mechanisms. In an extreme scenario, these different coexisting auctions could show negative interactions, where users participating in one of the auctions disrupt the other one.

This richer landscape where users care for ordering and privacy apart from inclusion raises concerns about the actual applicability of rigorous formal analyses like Tim Roughgarden's (cited above). In his paper, he shows that the EIP-1559 mechanism is Myopic Miner Incentive Compatible (MMIC, meaning that miners are incentivized to act according to it in the single-block scale), Off-Chain Agreement-proof (OCA-proof, meaning that users and miners cannot outgame the system by using off-chain communication), and, apart from periods of high-demand, User Incentive Compatible (UIC, meaning that it achieves the desired UX improvement of users expressing their true preferences for inclusion without needing to speculate on other users' actions). These conclusions rely however on the "purely inclusion" auction, and it's not clear how they would hold out in the current, more complex setting.

In particular, the paper discusses an alternative proposal, the "tipless mechanism", where there's no miner priority fee, and which is shown to be MMIC, always UIC, and OCA-proof apart from periods of

high demand. In short, it trades OCA-proofness for preserving the UX improvements throughout. The fact that, unlike what is suggested in the paper, Off-Chain Agreements are nowadays common via systems like Flashbots suggests that perhaps a tipless mechanism would have been a better choice than 1559's basefee + priority, optimizing the standard auction for regular users who only care about inclusion and directing more sophisticated users to ordering-focused auctions.

It is unfortunately extremely hard to rigorously model the ordering auction (consider for instance that the allocation rule cannot be simply expressed in terms of binary--included or not--values, or that the feasibility condition needs to take into account the interaction between transactions and hence cannot be expressed as a single inequality). Instead, it might be more useful to think of the different auctions separately and analyze their potential interactions, as pointed out before. To give one example of one such interaction we can take the case of μ, the marginal cost of including a transaction. In an MEV-less world this could be thought of as a constant, and has actually been [been estimated](). In the MEV-rich setting, however, a huge MEV reward present in the mempool might render it pointless to even run a regular auction for inclusion in the block, greatly raising greatly the value of μ, making it in turn impossible for users to converge on a reasonable value for the priority fee[^barnabenote].

To summarize, we have several kinds of auctions coexisting in Ethereum these days:

Auctioned good	Mechanism
Transaction inclusion	PGAs/EIP-1559 priority fees
Transaction privacy	Flashbots/Darkpools
Transaction ordering	Flashbots/Other relays

At Flashbots, we are considering making the auction mechanism more expressive to cover the use case of users that do not care about ordering but simply want front-running protection. Even the current [pricing formula]() might be biased to favor some kinds of extractions over others (arbitrages vs. liquidations in particular). As was pointed out above, this *de facto* tier system might not be optimal from a design perspective, considering it arose as a collage of actors trying to solve parts of the problem individually. In traditional finance, different instruments (stocks, options, etc.) have independent markets to accommodate their varying characteristics. It is an active area of research and a long term goal for Flashbots to craft a "Turing complete" auction where users can express arbitrary preferences in an efficient way[^auctions]. Ultimately, this calls for more discussion around the various coexisting auctions so that a more cohesive approach can be taken directly at the protocol level. This is particularly relevant in view of the upcoming changes needed for Ethereum 2.0.

Flashbots ethics

As stated above, Flashbots has introduced a way for searchers to express their transaction ordering preferences to miners, leading to a more efficient market all Ethereum users should ideally benefit from. In order to achieve this, Flashbots provides custom mining software (MEV-geth) to a number of miners jointly controlling the vast majority of Ethereum's hashrate (85% at the time of writing). This amounts to Flashbots having established an effective off-chain miner coordination mechanism, which naturally invites an exploration of its potentially nefarious implications. In particular, Flashbots has created a new Schelling point where miners can passively coordinate by adopting its software and defaults--not unlike geth before it.

When talking about miner coordination here we refer only to within-protocol coordination, that is, miner joint action that could be detrimental to the network but would still be admissible at the consensus level (i.e. no double spending, or otherwise disregarding the Ethereum protocol). True 51% attacks would severely damage the network, which is generally against the interest of miners. Instead, we focus on the more "benign" case where miners coordinate for their own benefit against other actors' interests, while abiding by the protocol rules. Short of analyzing how a focal point for miner coordination can affect the network (since, again, this was already available via geth upgrades), we ask the more specific question of whether the introduction of EIP-1559 increases the span of potentially nefarious consequences of Flashbots as a miner coordination mechanism.

We have already covered one way in which EIP-1559 changes the landscape, independently of Flashbots, by increasing the relative weight of MEV rewards within the total share of miner revenue. One way Flashbots affects this is via the share of block space dedicated to bundles as opposed to regular transactions, or the relative weight of the different auctions described in the previous section. MEV-geth has a setting for the maximum number of bundles considered for inclusion in a block, spawning a worker to build one template block for each number of bundles from 0 to this configurable maximum, and all template blocks are later compared for profitability. The larger this setting, the more profitable blocks might become, and the less block space left for standard user transactions. EIP-1559 incentivizing miners to go after more MEV might result in them being more accepting of higher and higher values, ultimately leading to MEV-only blocks. This scenario is however unlikely to play out, as there is an opportunity cost of including bundles by leaving transactions with high priority fees out. Altogether, we don't believe that EIP-1559 increases the risk of known nefarious behaviors facilitated by Flashbots.

EIP-1559, however, introduces a new undesirable behavior into consideration: miners coordinating to mine less-than-target sized blocks to drive the baseefee down to 0, which would effectively do away with the UX improvements that the EIP seeks to provide. Again, Flashbots is in a privileged position to enable this by providing an update that implements this behavior. More concretely, instead of including all transactions with gas limit above the basefee with greater than zero priority fee, the software could target a block size of $s_0 (1-\epsilon)$, where s_0 is the target block size and $\epsilon \in [0,1]$ is a parameter deliberately set to drive and keep the basefee down, dependent on the hashrate fraction running MEV-geth.

We leverage the Ethereum Foundation Robust Incentives Group's [framework]() to explore the viability of this attack (a notebook with the code for these results can be found [here]()). Taking a simple oscillatory demand scenario and setting $p_{FB}=0.85$ for the probability of the miner running MEV-geth, we simulate the system dynamics for different values of ϵ, illustrating how for a large enough value the basefee is driven to 0:

As in the previous case, there is an immediate economic downside for miners to go along with this strategy since they would be leaving money on the table with each block.

The next natural question to ask is how long would miners need to work at a loss until the drop in basefee finally compensates so that them colluding proves profitable. In simulations, we found this to be extremely sensitive to the nature of the demand, depending in particular on whether users would continue offering bids close to their true value or instead lower their bids by adapting to the new, artificially low basefee. While we cannot provide a meaningful answer until we see the EIP-1559 mechanism in action, we raise attention to the issue, while noting that even if such a collusion proves profitable after a short period of time, it could be broken at any point by a selfish miner including a larger number of transactions, and is thus not very likely to occur in practice.

Conclusions

We found no critical way in which EIP-1559 interacts with MEV extraction. However, we identified several areas where new dynamics might take place, in particular around miners' incentives to extract more MEV or defeat the new fee mechanism by passively colluding around a potential nefarious Flashbots' software update. Needless to say, it is not in the interest of Flashbots to provide such an update, but having 85% of Ethereum's hashrate running MEV-geth requires us to be thoughtful about the implications. Finally, we suggest that despite EIP-1559 being designed with a transaction inclusion auction in mind, many different auctions are nowadays taking place in Ethereum. It is critical to acknowledge this and design our systems to accommodate for these different auctions if we want to live up to Ethereum's open standards.

We would like to thank Barnabé Monnot and the Robust Incentives Group at the Ethereum Foundation, Leo Zhang, Tim Beiko, and Tina Zhen and the entire Flashbots team for conversations leading to the ideas presented here.

[^rev]: Realized Extractable Value is defined in our previous post on quantifying MEV extraction.

[^barnabenote]: Though see this note for an approach to bounding the uncle risk in an MEV-rich context.

[^numbersused]: At the time of writing, the values were calculated as follows:

$R_{E}= r_{\textrm{BLOCK REWARDS}} + r_{\textrm{TX FEES}} + r_{\textrm{MEV}} = 36,390,017\;\textrm{USD}$ and

$R_{1559}= r_{\textrm{BLOCK REWARDS}} + r_{\textrm{MEV}} = 31,327,517\;\textrm{USD}$, where:

$r_{\textrm{BLOCK REWARDS}}=13450\;\Xi\times P_{\textrm{ETH}}$,

$r_{\textrm{TX FEES}}=2250\; \Xi\times P_{\textrm{ETH}}$,

$r_{\textrm{MEV}} = 1,065,017\; \textrm{USD}$,

and $P_{\textrm{ETH}}= 2250\textrm{USD}$

[^xchains]: Dogecoin, Ethereum Classic, ZCash, Dash, Monero, Bitcoin Gold, and Verge were included for the calculations of chain X revenues.

[^basefee]: All else being equal, the basefee burning does not decrease Realized Extracted Value if we assume that the amount burned by the bundles will be equivalent to the one burned by the tail transactions that get pushed out of the block.

[^auctions]: Auction design is a rich field of study with many results focusing on computability of preferences/allocations, see Tim Roughgarden's lecture notes for an introduction.